

UNDER SEAL

UNITED STATES DISTRICT COURT FOR THE  
WESTERN DISTRICT OF NORTH CAROLINA  
CHARLOTTE DIVISION

FILED  
CHARLOTTE, NC

MAR 18 2015

U.S. DISTRICT COURT  
WESTERN DISTRICT OF NC

UNITED STATES OF AMERICA

v.

(1) VICTOR CHOSTAK

a/k/a "Victorchik"

a/k/a Viktor Shostak

(2)

(3) ALEXEY MARCHENKO

a/k/a "Buddha"

a/k/a "Gautama"

a/k/a Alexey Panov

a/k/a Alexey Pilyugin-Marchenko

a/k/a Oleksii Marchenko

(4)

DOCKET NO. 3:15cr 59-MOC

**BILL OF INDICTMENT**

**Violations:**

18 U.S.C. § 2

18 U.S.C. § 371

18 U.S.C. § 1028A

18 U.S.C. § 1029

18 U.S.C. § 1030

18 U.S.C. § 1956

18 U.S.C. § 2314

**UNDER SEAL**

**THE GRAND JURY CHARGES:**

At the specified times and at all relevant times:

**I. Introduction**

1. From in or about September 2007 and continuing until the present, an international money laundering organization, named Your Mule Cashout ("YMCO") by law enforcement, offered its money mule services to computer hackers, ultimately laundering at least \$10 million in stolen money from the United States overseas. Defendants VICTOR CHOSTAK, , ALEXEY MARCHENKO, and were members of YMCO from in or about July 2009 to at least in or about May 2011.

2. The defendants and others worked for YMCO primarily from Ukraine, but also from Germany, Poland, and other places outside the United States. They created, maintained, and

operated a sophisticated online infrastructure that allowed computer Hackers, who had stolen money primarily from United States companies' bank accounts, to conceal, transfer, and obtain the stolen money in countries outside of the United States.

3. With the assistance of YMCO Money Mules, YMCO members and other computer hackers electronically transferred millions in stolen money from U.S.-based compromised bank accounts to foreign countries, including Moldova, Ukraine, Russia, and Latvia.

## **II. The Fraudulent Scheme**

4. YMCO's services operated through an online infrastructure that allowed international cyber-criminals ("Hackers") to transfer stolen money out of the United States, primarily to Eastern Europe, in exchange for a percentage of the money stolen. YMCO marketed its services to these Hackers in underground chat forums.

5. These Hackers utilized various computer malware programs to infect the computers of United States companies. The malware programs enabled the Hackers to access the companies' bank accounts and then steal money from those accounts utilizing the services of YMCO.

6. YMCO provided these services to the Hackers through the use of Money Mules. Money Mules were U.S. residents whom YMCO deceived into believing that they were working for legitimate companies and conducting legitimate money transfers for those companies.

7. Through sophisticated computer programming, YMCO created seemingly legitimate websites for fake companies. YMCO members used these websites to recruit and employ Money Mules to conduct YMCO money laundering services. The websites, as well as the YMCO computer infrastructure, were created and maintained by "Programmers" and "Administrators," respectively.

8. After the creation of websites for the fake companies, YMCO "Recruiters" sent spam emails to potential Money Mules advertising employment opportunities. When a potential Money Mule responded to the spam, YMCO put the applicants through what appeared to be a legitimate hiring process, including an application, employment test, employment agreement, registration with the company's website, review of company policies, and assignment of a supervisor ("Handler"). YMCO Handlers were responsible for communicating directly with the Mules and assigning them money processing jobs. Handlers communicated with the Money Mules by email, telephone, and through a messaging platform built into the website of the fake company. Within YMCO, Recruiters and Handlers were supervised by "Managers," who reported directly to the YMCO Principals.

9. As a condition of employment, YMCO required each Money Mule to have a U.S.-based bank account and to provide the organization with their account information using a website associated with the fake company. YMCO informed the new Money Mules that they would be working from home, processing payments for legitimate transactions. Specifically, YMCO falsely represented that the Mules' job was to receive payments from businesses into their personal bank accounts, withdraw the money, and then wire the funds to the fake company's partners overseas. In reality, the Money Mules processed the Hackers' stolen proceeds and wired them out of the country to other YMCO conspirators.

10. Once YMCO obtained the Money Mules' account information, the organization made that information available to the Hackers through an online portal. After a Hacker compromised a bank account, the Hacker used the YMCO platform to access the account information for a Money Mule. The Hacker then sent the stolen money to the Mules' bank accounts.

11. At or around the time the Hackers wired money from the compromised account, a Handler emailed the relevant Money Mule alerting him that he had a new task. This caused the Mule to then log into the fake company website, where a message awaited. This message instructed the Mule to withdraw the newly deposited funds from his account, take the funds to a money services company, and transfer the funds overseas. In most instances, YMCO directed the funds to be wired by Western Union or MoneyGram to Eastern Europe, usually to Moldova, Ukraine, Russia, or Latvia.

12. YMCO and the Hackers used each Money Mule only once and never paid the promised salary. Sometimes the Money Mules lost money on the transaction because of associated banking and transmitting fees.

13. YMCO contracted with individuals ("Cash-Out Contractors") in the foreign countries to retrieve the wired money.

14. In addition to the United States, YMCO operated similar money laundering schemes in Germany, Italy, United Kingdom, and Australia, among other places.

### **III. Entities and Individuals**

15. *Defendants.* VICTOR CHOSTAK,  
ALEXEY MARCHENKO, and among others known and unknown,  
were members of YMCO:

- a. The defendant, VICTOR CHOSTAK, was a Ukrainian national who was at times a resident of Ukraine and the United States. CHOSTAK was a YMCO Manager from at least July 2009, and continuing to a date uncertain, but at least through May 2011. As a Manager, CHOSTAK recruited, hired, and managed the Money Mule Recruiters and Handlers. Specifically, CHOSTAK assigned tasks to Recruiters and Handlers;

provided domains for fake front company websites; provided facilities for communications, such as fax numbers, to Recruiters and Handlers to use with fake front companies; and worked with programmers to modify front company websites and various computer programs to meet the needs of Recruiters and Handlers. To hide his true identity, CHOSTAK used the moniker "Victorchik" while working for YMCO.

- b. The defendant, \_\_\_\_\_ was a Ukrainian national who was at times a resident of Ukraine and the Netherlands.

\_\_\_\_\_ was a YMCO Programmer from at least September 2009 and continuing to a date uncertain, but at least through March 2011. As a Programmer, \_\_\_\_\_ wrote computer programs that enabled YMCO conspirators to more effectively execute the scheme. To hide his true identity, \_\_\_\_\_ used the moniker \_\_\_\_\_ while working for YMCO.

- c. The defendant, ALEXEY MARCHENKO, was a Ukrainian national who was at times a resident of Ukraine and the Federal Republic of Germany. MARCHENKO was a YMCO Administrator from at least September 2009, and continuing to a date uncertain, but at least through April 2011. As an Administrator, MARCHENKO maintained and improved the functionality of YMCO's computer infrastructure. Specifically, MARCHENKO prepared and configured central servers; updated servers hosting the fake front company websites; updated and improved computer code; backed up databases that stored data for numerous YMCO computer

programs; and created and updated templates used to generate fake front companies. To hide his true identity, MARCHENKO used the monikers “Buddha” and “Gautama” while working for YMCO.

- d. The defendant, \_\_\_\_\_ was a Ukrainian national who was at times a resident of Ukraine and Poland. \_\_\_\_\_ was a YMCO Money Mule Recruiter from at least July 2009, and continuing to a date uncertain, but at least through May 2011. As a Recruiter, \_\_\_\_\_ created and edited recruiting email templates; sent recruiting emails to prospective Money Mules; communicated with prospective Mules; reported problems to management such as broken domains and fax numbers; and suggested changes to tools and processes to improve the recruitment of Money Mules. \_\_\_\_\_ used \_\_\_\_\_ as \_\_\_\_\_ moniker while working for YMCO.

16. *Money Mules.* As of July 2013, YMCO had recruited over 15,000 U.S.-based Money Mules to effectuate the transfer of stolen money from the United States to Eastern Europe, including the following individuals:

- a. M.C., who was during the relevant time period a resident Charlotte, North Carolina, within the Western District of North Carolina. M.C. accepted fake employment with a YMCO front company in or about July 2010 and held a bank account with SunTrust.
- b. M.P., who was during the relevant time period a resident of Clover, South Carolina. M.P. accepted fake employment with a YMCO front

company in or about April 2010 and held a bank account with Family Trust Federal Credit Union.

- c. C.L., who was during the relevant time period a resident of Wendell, North Carolina. C.L. accepted fake employment with a YMCO front company in or about March 2010 and held a bank account with RBC Centura.
- d. D.S., who was during the relevant time period a resident of Saxonburg, Pennsylvania. D.S. accepted fake employment with a YMCO front company in or about April 2010 and held a bank account with Woodforest Bank.
- e. C.M., who was during the relevant time period a resident of Las Cruces, New Mexico. C.M. accepted fake employment with a YMCO front company in or about October 2010 and held a bank account with Light Federal Credit Union.
- f. E.M., who was during the relevant time period a resident of Calvert City, Kentucky. E.M. accepted fake employment with a YMCO front company in or about March 2010 and held a bank account with Regions Bank.

17. *Victim Companies.* YMCO compromised over 750 U.S. bank accounts, most of which belonged to U.S. companies. YMCO and the Hackers generally gained access to these bank accounts by compromising the companies' computer systems, including the systems of the following victim companies:

- a. Victim Company #1, located in Beaumont, Texas with an account at Amegy Bank.

- b. Victim Company #2, located in Santa Rosa, California, with an account at Exchange Bank.
- c. Victim Company #3, located in Lubbock, Texas, with an account at First United Bank.
- d. Victim Company #4, located in Pocola, Oklahoma, with an account at First National Bank of Fort Smith.
- e. Victim Company #5, located in Byron Center, Michigan, with an account at Chemical Bank.

18. *Money Transfer Companies.* YMCO used the following companies to transfer stolen funds overseas:

- a. Western Union, a U.S.-based financial services company whose activities affect interstate and foreign commerce. Among other things, Western Union provided international money transfer services. The Western Union computer servers used to process the relevant electronic money transfers were located in the Western District of North Carolina. During the relevant time period, YMCO caused nearly 3,000 international money transfer wires of stolen funds to be sent through Western Union servers.
- b. MoneyGram, a U.S.-based financial service company whose activities affect interstate and foreign commerce. Among other things, MoneyGram provided international money transfer services. During the relevant time period, YMCO caused approximately 1,700 international money transfer wires of stolen funds to be sent through MoneyGram servers.



19. *Financial Institutions.* YMCO and the Hackers compromised accounts maintained at over 35 banks. The activities of these banks, including Bank of America, Amegy Bank, First United Bank, First National Bank of Fort Smith, Chemical Bank and Exchange Bank, affected interstate and foreign commerce.

**IV. Acts Committed in Furtherance of Illegal Conspiracy**

20. YMCO, through the Defendants and others, committed and caused to be committed the following acts in furtherance of the fraudulent scheme, within the Western District of North Carolina and elsewhere:

**RECRUITING AND HANDLING MONEY MULES**

21. On or about and between July and August 2009, Chostak trained new YMCO Mule Recruiters and Handlers by pretending to be a Money Mule, and sending them simulated email communications.

22. On or about August 26, 2010, using YMCO's internal communication forum, informed YMCO conspirators that he had created a report identifying Money Mules who had received spam emails from more than one fictitious front company.

23. On or about September 1, 2010, CHOSTAK, using YMCO's internal communication forum, suggested techniques that other YMCO Recruiters could use to increase the number of Mules recruited.

24. On or about December 20, 2010, CHOSTAK directed YMCO Recruiters to create new email templates to recruit Money Mules.

25. On or about December 22, 2010, using YMCO's internal communication forum, posted a new email template for recruiting potential Money Mules.

UPDATING FAKE FRONT COMPANY WEBSITES

26. From on or about and between March 8, 2010 and October 18, 2010, accepted assignments from YMCO to be the Mule Recruiter for approximately 18 fake front companies.

27. On or about August 17, 2010, using YMCO's internal communication forum, recommended improvements to the fake front company websites.

28. On or about August 19, 2010, using YMCO's internal communication forum, again recommended improvements to the fake front company websites.

29. On or about September 6, 2010, asked YMCO Programmers and Administrators to alter the fake front company websites to make it easier for Money Mules to register.

30. On or about September 8, 2010, using YMCO's internal communication forum, in response to tasking from YMCO, posted the URLs for legitimate job search websites in the United States, Italy, Hungary, Netherlands, Bulgaria, and United Kingdom.

31. On or about October 4, 2010, using YMCO's internal communication forum, reported that two domains associated with YMCO front company websites were not working.

32. On or about October 8, 2010, CHOSTAK, using YMCO's internal communication forum, directed other YMCO conspirators to search for potential new Money Mules in a legitimate commercial job website.

33. On or about October 14, 2010, using YMCO's internal communication forum, suggested that another YMCO Programmer add a security feature to

make the fake front company websites look more official and lower the risk of automated login attempts.

*HIRING OF COCONSPIRATORS TO WORK FOR YMCO*

34. On or about July 24, 2009, CHOSTAK recruited an individual to work for YMCO.

35. On or about July 27, 2009, CHOSTAK offered a job with YMCO as a Money Mule Recruiter.

36. On or about August 26, 2009, during the hiring process with YMCO, sent CHOSTAK her online contact information.

37. On or about September 2, 2010, CHOSTAK, using YMCO's internal communication forum, stated that YMCO had need for bilingual employees.

38. On or about September 20, 2010, MARCHENKO, using YMCO's internal communication forum, provided the name and contact information of a potential YMCO programmer who had rejected YMCO's offer of employment.

39. On or about October 14, 2010, using YMCO's internal communication forum, posted that he had interviewed two candidates for YMCO employment, and sent a job offer to a third applicant.

*REFINING SPAM EMAILS*

40. On or about November 9, 2009, CHOSTAK tested a YMCO Mule recruitment spam email template by sending himself a spam email.

41. On or about September 3, 2010, added additional spam templates to the computer program linked to Money Mule recruitment.

42. On or about October 25, 2010, \_\_\_\_\_ tasked a YMCO Programmer to update a computer program, linked to the spam emails, to make it more secure.

43. On or about November 4, 2010, \_\_\_\_\_, using YMCO's internal communication forum, discussed with another YMCO conspirator ways to make the spam emails reflect the recipient's gender.

IMPROVING FUNCTIONALITY OF COMPUTER PROGRAMS AND SYSTEMS

44. On or about September 3, 2009, \_\_\_\_\_ uploaded the computer code for the spam email application to a digital library that tracked the modification to that code.

45. On or about April 21, 2010, MARCHENKO modified a YMCO computer program that updated files on servers hosting fake front company websites.

46. On or about July 15, 2010, MARCHENKO modified a YMCO computer program that was used to generate fake front company websites.

47. On or about October 4, 2010, \_\_\_\_\_ modified a computer program that kept track of YMCO computers connected to the internet.

48. On or about and between October 7, 2010 and October 25, 2010, \_\_\_\_\_ logged into YMCO's central server numerous times to conduct the business of YMCO.

49. On or about and between October 12, 2010 and October 20, 2010, MARCHENKO logged into YMCO's central server numerous times to conduct the business of YMCO.

50. On or about and between 2010 and 2011, the exact dates being unknown, \_\_\_\_\_ repeatedly viewed and modified information in YMCO databases to maintain the functionality of the computer systems.

51. On or about and between 2010 and 2011, the exact date being unknown, MARCHENKO copied the computer code for one front company website from one YMCO server to another.

52. On or about and between 2010 and 2011, the exact date being unknown, MARCHENKO, executed computer code that synched files across the YMCO computer network.

53. On or about and between 2010 and 2011, the exact dates being unknown, MARCHENKO, created backups of databases that contained the information for eight fake front companies.

54. On or about and between 2010 and 2011, the exact date being unknown, MARCHENKO, restarted the program that controlled YMCO emails processed on YMCO's main server.

55. On or about and between 2010 and 2011, the exact dates being unknown, MARCHENKO viewed and modified information in YMCO databases to maintain the functionality of the computer systems.

THEFT AND MONEY LAUNDERING OF VICTIM FUNDS

*Theft of Funds from Victim Company #1*

56. On or about July 13, 2010, a YMCO Recruiter "hired" M.C. to work as a Money Mule for a fake front company that M.C. believed to be a legitimate company known as "GNB Group, Inc."

57. On or about August 2, 2010, the exact date being unknown, a Hacker using the moniker "fuckthisworld" compromised Victim Company #1's computer system, thereby giving the Hacker unauthorized access to the company's online bank account with Amegy bank.

58. On or about August 2, 2010, Hacker “fuckthisworld” used YMCO software to select YMCO Money Mule M.C. to receive a fraudulent transfer of funds from Victim Company #1’s account, and then transferred said funds to M.C. As part of this process, YMCO transferred M.C.’s personal information to the Hacker, including, but not limited to, M.C.’s full name, date of birth, bank account number, and routing number.

59. On or about August 2, 2010, Hacker “fuckthisworld” fraudulently transferred \$7,356 from Victim Company #1’s account to Money Mule M.C.’s account at SunTrust bank.

60. On or about August 2, 2010, a YMCO Handler, using the alias “Linda Sprinks,” instructed Money Mule M.C. to withdraw funds that had been transferred into M.C.’s bank account and transfer them overseas through Western Union and MoneyGram to Moldova and Ukraine.

61. On or about August 2, 2010, in accordance with YMCO’s tasking, Money Mule M.C. withdrew the funds from M.C.’s bank account and used Western Union and MoneyGram to send separate wires to conspirators in Moldova and Ukraine. Specifically, M.C. wired \$2,255 through Western Union to “Anna Sergheiciuc” in Moldova and \$2,250 to “Damir Mamedov” in Ukraine. M.C. also wired \$2,260 through MoneyGram to “Anatoliy Melnychuk” in Ukraine.

*Theft of Funds from Victim Company #3*

62. On or about April 19, 2010, a YMCO Recruiter “hired” M.P. to work as a Money Mule for a fake front company that M.P. believed to be a legitimate company known as “Wave Group, Inc.”

63. On or about May 7, 2010, the exact date being unknown, a Hacker using the moniker “ibn” compromised Victim Company #3’s computer system, thereby giving the Hacker unauthorized access to the company’s online bank account with First United bank.

64. On or about May 7, 2010, Hacker "ibn" used YMCO software to select YMCO Money Mule M.P. to receive a fraudulent transfer of funds from Victim Company #3's account, and then transferred said funds to M.P. As part of this process, YMCO transferred M.P.'s personal information to the Hacker, including, but not limited to, M.P.'s full name, date of birth, bank account number, and routing number.

65. On or about May 7, 2010, Hacker "ibn" fraudulently transferred \$9,400 from Victim Company #3's account to Money Mule M.P.'s account at Family Trust Federal Credit Union.

66. On or about May 7, 2010, a YMCO Handler, using the alias "Tiffany Glide," instructed Money Mule M.P. to withdraw funds that had been transferred into M.P.'s bank account and transfer them overseas through Western Union to Ukraine.

67. On or about May 7, 2010, in accordance with YMCO's tasking, Money Mule M.P. withdrew \$9,400 from M.P.'s bank account and used Western Union and MoneyGram to send separate wires to conspirators in Moldova and Ukraine. Specifically, M.P. wired \$2,880 through Western Union to "Artem Ohruschak" in Ukraine and \$2,882 to "Inga Ciora" in Moldova. M.P. also wired \$2,884 through MoneyGram to "Andrei Arnaut" in Moldova.

*Theft of Funds from Victim Company #4*

68. On or about March 2010, a YMCO Recruiter "hired" C.L. to work as a Money Mule for a fake front company that C.L. believed to be a legitimate company known as "Point Group, Inc."

69. On or about April 6, 2010, the exact date being unknown, a Hacker using the moniker "Harman" compromised Victim Company #4's computer system, thereby giving the

Hacker unauthorized access to the company's online bank account with First National Bank of Fort Smith.

70. On or about April 6, 2010, a Hacker "Harman" used YMCO software to select YMCO Money Mule C.L. to receive a fraudulent transfer of funds from Victim Company #4's account, and then transferred said funds to C.L. As part of this process, YMCO transferred C.L.'s personal information to the Hacker, including, but not limited to, C.L.'s full name, date of birth, bank account number, and routing number.

71. On or about April 6, 2010, Hacker "Harman" fraudulently transferred \$9,800 from Victim Company #4's account to Money Mule C.L.'s account at RBC Centura bank.

72. On or about April 6, 2010, a YMCO Handler, using the alias "Pamela Payton," instructed Money Mule C.L. to withdraw funds that had been transferred into C.L.'s bank account and transfer the funds overseas through Western Union and MoneyGram to Moldova and Ukraine.

73. On or about April 6, 2010, in accordance with YMCO's tasking, Money Mule C.L. withdrew \$9,800 from C.L.'s bank account and used Western Union and MoneyGram to send separate wires to conspirators in Moldova and Ukraine. Specifically, C.L. wired \$2,980 through Western Union to "Simion Tavaluc" and \$2,970 to "Vitali Cosaciov" in Moldova. C.L. also wired \$3,065 through MoneyGram to "Olga Banschikova" in Ukraine.

*Second Theft of Funds from Victim Company #3*

74. On or about April 19, 2010, a YMCO Recruiter "hired" D.S. to work as a Money Mule for a fake front company that D.S. believed to be a legitimate company known as "Wave Group, Inc."



75. On or about May 7, 2010, the exact date being unknown, a Hacker believed to use the moniker "ibn" compromised victim company Victim Company #3's computer system, thereby giving the Hacker unauthorized access to the company's online bank account with First United Bank.

76. On or about May 7, 2010, Hacker "ibn" used YMCO software to select YMCO Money Mule D.S. to receive a fraudulent transfer of funds from Victim Company #3's account, and then transferred said funds to D.S. As part of this process, YMCO transferred D.S.'s personal information to the Hacker, including, but not limited to, D.S.'s full name, date of birth, bank account number, and routing number.

77. On or about May 7, 2010, Hacker "ibn" fraudulently transferred \$7,400 from Victim Company #3's account to Money Mule D.S.'s account at Woodforest Bank.

78. On or about May 7, 2010, a conspiracy YMCO Handler, using the alias "Tiffany Glide," instructed Money Mule D.S. to withdraw funds that had been transferred into D.S.'s bank account and transfer the funds overseas through Western Union and MoneyGram to Ukraine.

79. On or about May 7, 2010, in accordance with YMCO's tasking, Money Mule D.S. withdrew \$7,400 from D.S.'s bank account and used Western Union and MoneyGram to send separate wires to conspirators in Moldova and Ukraine. Specifically, D.S. wired \$2,269 through Western Union to "Elena Mikhalkina" and \$2,260 to "Ruslan Zhumanazarov" in Ukraine. D.S. also wired \$2,278 through MoneyGram to "Ekaterina Merkulova" in Ukraine.

*Theft of Funds from Victim Company #5*

80. On or about October 13, 2010, a YMCO Recruiter "hired" C.M. to work as a Money Mule for a fake front company that C.M. believed to be a legitimate company known as "Vidi Group, Inc."

81. On or about October 20, 2010, the exact date being unknown, a Hacker believed to use the moniker “ibn” compromised Victim Company #5’s computer system, thereby giving the Hacker unauthorized access to the company’s online bank account with Chemical Bank.

82. On or about October 20, 2010, Hacker “ibn” used YMCO software to select YMCO Money Mule C.M. to receive a fraudulent transfer of funds from Victim Company #5’s account, and then transferred said funds to C.M. As part of this process, YMCO transferred C.M.’s personal information to the Hacker, including, but not limited to, C.M.’s full name, date of birth, bank account number, and routing number.

83. On or about October 21, 2010, Hacker “ibn” fraudulently transferred \$4,950 from Victim Company #5’s account to Money Mule C.M.’s account at Light Federal Credit Union.

84. On or about October 21, 2010, a YMCO Handler, using the alias “Suzan Whats,” instructed Money Mule C.M. to withdraw funds that had been transferred into C.M.’s bank account and transfer the funds overseas through Western Union and MoneyGram to Moldova and Ukraine.

85. On or about October 21, 2010, in accordance with YMCO’s tasking, Money Mule C.M. withdrew \$4,950 from C.M.’s bank account and used Western Union and MoneyGram to send separate wires to conspirators in Moldova and Ukraine. Specifically, C.M. wired \$2,270 through Western Union to “Alexei Nudenenco” in Moldova. C.M. also wired \$2,284 through MoneyGram to “Petro Karaykoza” in Ukraine.

*Theft of Funds from Victim Company #2*

86. On or about March 12, 2010, a YMCO Recruiter “hired” E.M. to work as a Money Mule for a fake front company that E.M. believed to be a legitimate company known as “Optimus Group, Inc.”

87. On or about March 19, 2010, the exact date being unknown, a Hacker believed to use the moniker "Harman" compromised victim company Victim Company #2's computer system, thereby giving the Hacker unauthorized access to the company's online bank account with Exchange Bank.

88. On or about March 19, 2010, Hacker "Harman" used YMCO software to select YMCO Money Mule E.M. to receive a fraudulent transfer of funds from Victim Company #2's account, and then transferred said funds to E.M. As part of this process, YMCO transferred E.M.'s personal information to the Hacker, including, but not limited to, E.M.'s full name, date of birth, bank account number, and routing number.

89. On or about March 19, 2010, Hacker "Harman" fraudulently transferred \$8,291 from Victim Company #2's account to Money Mule E.M.'s account at Regions Bank.

90. On or about March 19, 2010, a YMCO Handler, using the alias "Ronald Quisano," instructed Money Mule E.M. to withdraw funds that had been transferred into E.M.'s bank account and transfer the funds overseas through Western Union and MoneyGram to Moldova and Ukraine.

91. On or about March 19, 2010, in accordance with YMCO's tasking, Money Mule E.M. withdrew approximately \$8,291 from E.M.'s bank account and used Western Union and MoneyGram to send separate wires to conspirators in Moldova and Ukraine. Specifically, E.M. wired \$2,977 through Western Union to "Igor Gonta" in Moldova and \$2,500 "Oleksiy Piskunov" in Ukraine. E.M. also wired \$2,150 through MoneyGram to "Alla Turkina" in Ukraine.

**COUNT ONE**  
**(Conspiracy to Commit Money Laundering)**

92. Paragraphs 1 through 91 are realleged and incorporated by reference here.

93. Beginning in or about July 2009, and continuing to at least in or about May 2011, in the Western District of North Carolina and elsewhere, the defendants, VICTOR CHOSTAK, ALEXEY MARCHENKO, and did knowingly and intentionally conspire and agree with each other and others known and unknown to the Grand Jury to commit offenses against the United States in violation of 18 U.S.C. §§ 1956 and 1957, to wit:

- a. to knowingly conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is, (i) conspiracy to commit fraud in relation to computers in violation of 18 U.S.C. §§ 371 and 1030(b); (ii) conspiracy to transport stolen property in violation of 18 U.S.C. §§ 371 and 2314; (iii) conspiracy to commit access device fraud in violation of 18 U.S.C. § 1029(b)(2); and (iv) interstate transportation of stolen property in violation of 18 U.S.C. § 2314, knowing that the transactions were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of such specified unlawful activity, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some unlawful activity, in violation of 18 U.S.C. § 1956(a)(1)(B)(i);

- b. to transport, transmit, and transfer, and attempt to transport, transmit, and transfer a monetary instrument and funds involving the proceeds of specified unlawful activity, that is, (i) conspiracy to commit fraud in relation to computers in violation of 18 U.S.C. §§ 371 and 1030(b); (ii) conspiracy to transport stolen property in violation of 18 U.S.C. §§ 371 and 2314; (iii) conspiracy to commit access device fraud in violation of 18 U.S.C. § 1029(b)(2); and (iv) interstate transportation of stolen property in violation of 18 U.S.C. § 2314, from a place in the United States to or through a place outside the United States, knowing that the funds involved in the transportation, transmission, and transfer represented the proceeds of some unlawful activity and knowing that such transportation, transmission, and transfer was designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of such specified unlawful activity, in violation of 18 U.S.C. § 1956(a)(2)(B)(i); and
- c. to knowingly engage and attempt to engage in a monetary transaction by, through, and to a financial institution, affecting interstate and foreign commerce, in criminally derived property of a value greater than \$10,000, that is, the withdrawal, deposit, and transfer of U.S. currency, funds, and monetary instruments, such property having been derived from specified unlawful activity, that is, (i) conspiracy to commit fraud in relation to computers in violation of 18 U.S.C. §§ 371 and 1030(b); (ii) conspiracy to transport stolen property in violation of 18 U.S.C. §§ 371 and 2314;

(iii) conspiracy to commit access device fraud in violation of 18 U.S.C. § 1029(b)(2); and (iv) interstate transportation of stolen property in violation of 18 U.S.C. § 2314, in violation of 18 U.S.C. § 1957(a).

**MANNER AND MEANS**

94. The manner and means used to accomplish the objectives of the conspiracy included, among others, those described in Paragraphs 1 through 14.

**OVERT ACTS**

95. In furtherance of the conspiracy, and to effect its objects and purposes, various overt acts were committed by the defendants and their conspirators known and unknown to the Grand Jury, in the Western District of North Carolina and elsewhere, including but not limited to the acts described in Paragraphs 1 through 91.

All in violation of 18 U.S.C. § 1956(h).

**COUNTS TWO THROUGH TWELVE**  
**(Money Laundering)**

96. Paragraphs 1 through 91 are realleged and incorporated by reference here.

97. On or about each of the dates below, within the Western District of North Carolina, and elsewhere, the defendants, VICTOR CHOSTAK, ALEXEY MARCHENKO, and , aiding and abetting each other and others known and unknown to the Grand Jury, attempted to and did transport, transmit, and transfer a monetary instrument and funds involving the proceeds of specified unlawful activity, that is, (a) conspiracy to commit fraud in relation to computers in violation of 18 U.S.C. §§ 371 and 1030(b); (b) conspiracy to transport stolen property in violation of 18 U.S.C. §§ 371 and 2314; (c) conspiracy to commit access device fraud in violation of 18 U.S.C. § 1029(b)(2); and (d) interstate transportation of stolen property in violation of 18 U.S.C. § 2314, from a place in the United States, through Western Union servers located in the Western District of North Carolina, to or through a place outside the United States, knowing that the funds involved in the transportation, transmission, and transfer represented the proceeds of such unlawful activity and knowing that such transportation, transmission, and transfer was designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of such specified unlawful activity, each instance identified below being a separate violation of 18 U.S.C. §§ 1956(a)(2)(B)(i) and 2:

| COUNT | APPROXIMATE DATE | MONETARY TRANSACTION   |
|-------|------------------|--|
| TWO   | March 19, 2010   | International money transfer of \$2,977 sent by Money Mule E.M. to a conspirator located in Chisinau, Moldova. |
| THREE | March 19, 2010   | International money transfer of \$2,500 sent by Money Mule E.M. to a conspirator located in Kiev, Ukraine.     |

| COUNT  | APPROXIMATE DATE | MONETARY TRANSACTION   |
|--------|------------------|--|
| FOUR   | April 6, 2010    | International money transfer of \$2,970 sent by Money Mule C.L. to a conspirator located in Chisinau, Moldova. |
| FIVE   | April 6, 2010    | International money transfer of \$2,980 sent by Money Mule C.L. to a conspirator located in Chisinau, Moldova. |
| SIX    | May 7, 2010      | International money transfer of \$2,269 sent by Money Mule D.S. to a conspirator located in Mariupol, Ukraine. |
| SEVEN  | May 7, 2010      | International money transfer of \$2,260 sent by Money Mule D.S. to a conspirator located in Kiev, Ukraine.     |
| EIGHT  | May 7, 2010      | International money transfer of \$2,882 sent by Money Mule M.P. to a conspirator located in Chisinau, Moldova. |
| NINE   | May 7, 2010      | International money transfer of \$2,880 sent by Money Mule M.P. to a conspirator located in Odessa, Ukraine.   |
| TEN    | August 2, 2010   | International money transfer of \$2,255 sent by Money Mule M.C. to a conspirator located in Chisinau, Moldova. |
| ELEVEN | August 2, 2010   | International money transfer of \$2,250 sent by Money Mule M.C. to a conspirator located in Donetsk, Ukraine.  |
| TWELVE | October 21, 2010 | International money transfer of \$2,270 sent by Money Mule C.M. to a conspirator located in Leova, Moldova.    |



**COUNT THIRTEEN**  
**(Conspiracy to Commit Computer Fraud)**

98. Paragraphs 1 through 91 are realleged and incorporated by reference herein.

99. Beginning in or about July 2009, and continuing to at least in or about May 2011, in the Western District of North Carolina and elsewhere, the defendants, VICTOR CHOSTAK, ALEXEY MARCHENKO, and , did knowingly and intentionally conspire and agree with each other and others known and unknown to the Grand Jury to commit offenses against the United States in violation of 18 U.S.C. § 1030, to wit: to knowingly, and with intent to defraud, access a protected computer without authorization, and by means of such conduct to further the intended fraud and obtain anything of value, the value of which exceeded \$5,000 during a one-year period, in violation of 18 U.S.C. § 1030(a)(4).

**MANNER AND MEANS**

100. The manner and means used to accomplish the objectives of the conspiracy included, among others, those described in Paragraphs 1 through 14.

**OVERT ACTS**

101. In furtherance of the conspiracy, and to effect its objects and purposes, various overt acts were committed by the defendants and their co-conspirators known and unknown to the Grand Jury, in the Western District of North Carolina and elsewhere, including but not limited to the acts described in Paragraphs 1 through 91.

All in violation of 18 U.S.C. §§ 371 and 1030(b).

**COUNT FOURTEEN**  
**(Conspiracy to Transport Stolen Property)**

102. Paragraphs 1 through 91 are realleged and incorporated by reference herein.

103. Beginning in or about July 2009, and continuing to at least in or about May 2011, in the Western District of North Carolina and elsewhere, the defendants, VICTOR CHOSTAK, ALEXEY MARCHENKO, and did knowingly and intentionally conspire and agree with each other and others known and unknown to the Grand Jury to commit offenses against the United States in violation of 18 U.S.C. § 2314, to wit: to transport, transmit, and transfer in interstate and foreign commerce United States money over \$5,000, knowing the money to have been stolen and taken by fraud in violation of 18 U.S.C. § 2314.

**MANNER AND MEANS**

104. The manner and means used to accomplish the objectives of the conspiracy included, among others, those described in Paragraphs 1 through 14.

**OVERT ACTS**

105. In furtherance of the conspiracy, and to effect its objects and purposes, various overt acts were committed by the defendants and their conspirators known and unknown to the Grand Jury, in the Western District of North Carolina and elsewhere, including but not limited to the acts described in Paragraphs 1 through 91.

All in violation of 18 U.S.C. § 371.

**COUNT FIFTEEN**  
**(Conspiracy to Commit Access Device Fraud)**

106. Paragraphs 1 through 91 are realleged and incorporated by reference herein.

107. Beginning in or about July 2009, and continuing to at least in or about May 2011, in the Western District of North Carolina and elsewhere, the defendants, VICTOR CHOSTAK, , ALEXEY MARCHENKO, and did knowingly and intentionally conspire and agree with each other and others known and unknown to the Grand Jury to commit offenses against the United States in violation of 18 U.S.C. § 1029, to wit: to knowingly and with intent to defraud traffic in and use one or more unauthorized access devices during any one year period, and by such conduct obtain anything of value aggregating \$1,000 or more during that period, in violation of 18 U.S.C. § 1029(a)(2).

**MANNER AND MEANS**

108. The manner and means used to accomplish the objectives of the conspiracy included, among others, those described in Paragraphs 1 through 14.

**OVERT ACTS**

109. In furtherance of the conspiracy, and to effect its objects and purposes, various overt acts were committed by the defendants and their conspirators known and unknown to the Grand Jury, in the Western District of North Carolina and elsewhere, including but not limited to the acts described in Paragraphs 1 through 91.

All in violation of 18 U.S.C. § 1029(b)(2).

**COUNTS SIXTEEN THROUGH NINETEEN**  
**(Interstate and Foreign Transportation of Stolen Property)**

110. Paragraphs 1 through 91 are realleged and incorporated by reference herein.

111. On or about the dates below, within the Western District of North Carolina, and elsewhere, the defendants, VICTOR CHOSTAK, ALEXEY MARCHENKO, and aiding and abetting each other and others known and unknown to the Grand Jury, attempted to and did transport, transmit, and transfer in interstate and foreign commerce United States money over \$5,000, knowing the money to have been stolen and taken by fraud in violation of 18 U.S.C. § 2314, each instance identified below being a separate violation of 18 U.S.C. §§ 2314 and 2:

| COUNT     | APPROXIMATE DATE | TRANSPORTATION OF<br>STOLEN MONEY   |
|-----------|------------------|---|
| SIXTEEN   | March 19, 2010   | International money transfers of approximately \$5,477 of stolen money conducted by Money Mule E.M. through Western Union servers located in the Western District of North Carolina to conspirators located in Chisinau, Moldova and Kiev, Ukraine. |
| SEVENTEEN | April 6, 2010    | International money transfers of approximately \$5,950 of stolen money conducted by Money Mule C.L. through Western Union servers located in the Western District of North Carolina to conspirators located in Chisinau, Moldova.                   |
| EIGHTEEN  | May 7, 2010      | International money transfer of approximately \$5,762 conducted by Money Mule M.P. through Western Union servers located in the Western District of North Carolina to conspirators located in Chisinau, Moldova and Odessa, Ukraine.                |

| COUNT    | APPROXIMATE DATE | TRANSPORTATION OF<br>STOLEN MONEY  |
|----------|------------------|--|
| NINETEEN | August 2, 2010   | Interstate money transfer of approximately \$7,356 of stolen money sent from Texas to the Western District of North Carolina and received by Money Mule M.C. |

**COUNTS TWENTY THROUGH TWENTY-FIVE**  
**(Aggravated Identity Theft)**

112. Paragraphs 1 through 91 are realleged and incorporated by reference here.

113. On or about each of the dates below, within the Western District of North Carolina, and elsewhere, the defendants, VICTOR CHOSTAK, ALEXEY MARCHENKO, and aiding and abetting each other and others known and unknown to the Grand Jury, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, to wit, the full name, date of birth, bank account number, and routing number of each Money Mule listed below, during and in relation to the offenses charged in Counts Thirteen and Fifteen, knowing that the means of identification belonged to an actual person, each instance identified below being a separate violation of 18 U.S.C. §§ 1028A(a)(1) and 2:

| COUNT        | APPROXIMATE DATE | MONEY MULE |
|--------------|------------------|------------|
| TWENTY       | March 19, 2010   | E.M.       |
| TWENTY-ONE   | April 6, 2010    | C.L.       |
| TWENTY-TWO   | May 7, 2010      | D.S.       |
| TWENTY-THREE | May 7, 2010      | M.P.       |
| TWENTY-FOUR  | August 2, 2010   | M.C.       |
| TWENTY-FIVE  | October 20, 2010 | C.M.       |

### **NOTICE OF FORFEITURE**

114. Paragraphs 1 through 113 are realleged and incorporated by reference here for the purpose of alleging forfeiture, pursuant to 18 U.S.C. §§ 981, 982, and 1030; 21 U.S.C. § 853; and 28 U.S.C. § 2461.

115. Pursuant to Federal Rule of Criminal Procedure 32.2(a), the United States gives notice to each defendant that, in the event of a conviction of any of the offenses charged in this Indictment, the United States intends to forfeit property as further described in this notice.

116. If a defendant is convicted of conspiracy to commit fraud in connection with computers, in violation of 18 U.S.C. §§ 371 and 1030, then the following property shall be subject to forfeiture: any personal property that was used or intended to be used to commit or to facilitate the commission of such violation, and any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation, pursuant to 18 U.S.C. §§ 1030(i)(1) and (j); any property constituting, or derived from, proceeds the defendant obtained directly or indirectly, as the result of such violation, pursuant to 18 U.S.C. § 982(a)(2)(B), and any property, real or personal, which constitutes or is derived from proceeds traceable to the violation, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c).

117. If a defendant is convicted of conspiracy to commit access device fraud, in violation of 18 U.S.C. § 1029(b)(2), then the following property shall be subject to forfeiture: any property constituting, or derived from, proceeds the person obtained directly or indirectly, as the result of such violation, pursuant to 18 U.S.C. § 982(a)(2)(B), and any property, real or personal, which constitutes or is derived from proceeds traceable to the violation of § 1029, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c).

118. If a defendant is convicted of conspiracy to transport stolen property, in violation of 18 U.S.C. § 371, or interstate transportation of stolen property, in violation of 18 U.S.C. § 2314, then the following property shall be subject to forfeiture: any property, real or personal, which constitutes or is derived from proceeds traceable to the violation, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c).

119. If a defendant is convicted of conspiracy to commit money laundering or money laundering, in violation of 18 U.S.C. § 1956, then the following property shall be subject to forfeiture: any property, real or personal, involved in such offense, or any property traceable to such property, pursuant to 18 U.S.C. § 982(a)(1); and any property, real or personal, involved in a transaction or attempted transaction in violation of § 1956, or any property traceable to such property, pursuant to 18 U.S.C. § 981(a)(1)(A) and 28 U.S.C. § 2461(c).

120. If any of the property described above, as a result of any act or omission of the defendant:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;



the United States shall be entitled to and intends to seek forfeiture of substitute property pursuant to 21 U.S.C. § 853(p), as incorporated by 28 U.S.C. § 2461(c).

121. The Grand Jury finds probable cause to believe that the following property is subject to forfeiture on one or more of the grounds stated above: a forfeiture money judgment in the amount of approximately \$10,000,000, such amount constituting the proceeds of the violations set forth in this Bill of Indictment.

All pursuant to 18 U.S.C. §§ 981, 982, and 1030; 21 U.S.C. § 853; and 28 U.S.C. § 2461.

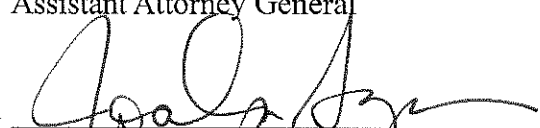
A TRUE BILL


DATE: 3/18/15

JILL WESTMORELAND ROSE  
ACTING UNITED STATES ATTORNEY

  
\_\_\_\_\_  
KEVIN ZOLOT  
Assistant United States Attorney

LESLIE R. CALDWELL  
Assistant Attorney General

  
\_\_\_\_\_  
JOCELYN AQUINO  
Trial Attorney

  
\_\_\_\_\_  
RYAN K. DICKEY  
Trial Attorney  
U.S. Department of Justice, Criminal Division  
Computer Crime and Intellectual Property Section